AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.-3. (canceled)

4. (currently amended) A method according to claim ~~1~~32, in which each data frame includes a frame identity field, and each key generated by the secure module is specific to one frame identified by the said field.

5. (currently amended) A method according to claim ~~1~~32, in which the step of distributing multiple copies of the said data comprises multicasting packets of data via a communications network to the plurality of users.

6. (currently amended) A method according to claim ~~1~~32, in which the control message is distributed with a data frame to the multiplicity of users, a user identity field identifying a selected user or group of users is included in the control message, and the control message is acted on only by the user or group of users identified by the said user identity field.

7. (currently amended) A method according to claim ~~1~~32, in which the control message includes a stop flag, and in response to the stop flag the generation of keys at the or each selected user is stopped.

8. (currently amended) A method according to claim ~~1~~32, including returning a response signal from the secure module to the source of the control message.

9. (original) A method according to claim 8, in which the control message includes a contact sender flag, and the step of returning a response signal from the secure module is carried out when the contact sender flag is set.

10. (previously presented) A method according to claim 8, including transmitting a further control message to the user on receipt of the said response signal.

11. (canceled)

12. (previously presented) A data communications system comprising:

a) a remote data source arranged to output a plurality of frames;

b) encryption means for encrypting the plurality of frames with different respective keys;

c) a communications channel arranged to distribute multiple copies of the encrypted data frames, each with a control field;

d) a multiplicity of customer terminals arranged to receive from the communications channel respective copies of the encrypted data frames with the control fields;

e) a key generator located at a customer terminal and programmed to generate from a seed value keys for use in decrypting data frames;

f) key control means connected to the key generator, the key control means comprising:

an interface for receiving the control fields ; and

control means arranged to only release keys for decrypting those respective frames for which a control field is received and being arranged to, in response to the said

control messages in the control fields, control the availability to the user of keys generated from the seed value; and

g) decryption means connected to the key generator and arrange to decrypt the data frames received at the customer terminal from the communications channel.

13. (original) A data communications system according to claim 12, in which the communications channel is a packet-switched data network.

14. (currently amended) A customer terminal for use in a method according to claim ~~1~~32, the customer terminal comprising:

a) a data interface for connection to a data communications channel;

b) a key generator programmed to generate from a seed value keys for use in decrypting data frames:

c) decryption means connected to the data interface and the key generator and arranged to decrypt data frames received via the data interface; and

d) key control means connected to the key generator, the key control means comprising:

an interface for receiving control fields; and

control means arrange to only release keys for decrypting those respective data frames received with a control field;

the control means being arranged to in response to control messages in the control fields, control the availability to the user keys generated from the seed value.

15. (currently amended) A data server for use in method according to claim ~~1~~32, the data server comprising:

a) a data interface for connection to a data communications channel;

b) means for outputting encrypted data frames with control fields via the data interface onto the communications channel for receipt by a multiplicity of customer terminals;

c) means for outputting the control fields having control messages onto a data communications channel for controlling the operation of key generators at customer terminals.

16. (currently amended) A method according to claim ~~1~~32, including generating keys from the seed value by iterated operations on the seed value by selected ones of a plurality of predetermined functions.

17-20. (canceled)

21. (currently amended) A method according to claim ~~1~~32, including applying different characteristic variations to data decrypted at different respective customer terminals.

22. (currently amended) A method according to claim ~~1~~32, including a plurality of remote data sources, each outputting a respective plurality of frames.

23. (previously presented) A method according to claim 22, in which the customer terminal receives a primary seed value common to different respective data streams from the plurality of data sources, and derives from the common primary key a plurality of

different respective secondary seed values for decrypting frames from different respective data sources.

24. (previously presented) A method according to claim 23, in which data received from different data sources includes different respective source identity values, and the respective secondary seed value is generated from the primary seed value by modifying the primary seed value with the source identity value.

25. (currently amended) A method according to claim ~~1~~32, in which each data frame includes a frame type field.

26. (original) A method according to claim 25, including storing a receipt including data from the frame type field.

27-28. (canceled)

29. (currently amended) A method as in claim ~~1~~32, wherein the control message received by the secure module causes the secure module to cease releasing keys.

30. (currently amended) A method as in claim ~~11~~33, wherein the control message received by the secure module causes the secure module to cease releasing keys.

31. (previously presented) A data communications system as in claim 12, wherein the control message received by the key control means causes the key control means to cease releasing keys.

32. (currently amended) A method of distributing digitally encoded data, comprising:

a) dividing said data into a multiplicity of frames,

b) encrypting said frames,

c) distributing multiple copies of the said data frames to a multiplicity of users, each frame being distributed with a control field,

d) communicating a seed value for key generation to respective secure modules located at each of the multiplicity of users,

e) decrypting the data frames at respective users using keys derived from the seed value communicated to the secure module, the secure module being arranged to enable decryption of a respective frame only when said control field has been passed to the secure module,

f) passing a control message, for modifying and controlling the availability of keys, in the control field to the secure module at a selected one or more users, and

g) at the secure module of the or each selected user, in response to the said control message, controlling the availability of keys generated from the said seed value, thereby controlling access by the users to the said data;

~~A method as in claim 1,~~ wherein each of the frames is encrypted with a different key.

33. (currently amended) A method of operating a customer terminal in a data communications system, the method comprising:

a) receiving at the customer terminal a multiplicity of encrypted data frames, each with a control field;

b) receiving at the customer terminal a seed value for key generation;

c) passing the said seed value for key generation to a secure module located at the customer terminal;

d) generating in the secure module using the seed value keys for the decryption of data frames;

e) decrypting using the said keys only those respective data frames for which a control field has been received;

f) passing to the said secure module a control message received in the control field; and

g) in response to the said control message, controlling the availability of keys generated using the said seed value and thereby controlling access by the user of the customer terminal to data received at the customer terminal;

~~A method as in claim 11,~~ wherein each of the frames is encrypted with a different key.